What is claimed is:

1. A method for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, the method comprising:

receiving, from the certification authority in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the identity of the end user, and a proof of identity possession by the end user;

analyzing the content of said plurality of data fields;

verifying the accuracy of said plurality of data fields; and

if said plurality of data fields is verified as accurate, sending a signed object to the certification authority, said signed object comprising the proof of possession confirmation.

2. The method of claim 1, wherein said plurality of data fields further comprises:

a host name;

a subject identification;

a subject public key information; and

a sealed proof of possession.

3. The method of claim 2, wherein analyzing the content of said plurality of data fields further comprises:

decrypting a proof of possession structure from said sealed proof of possession;

extracting a password from said sealed proof of possession structure;

extracting a key identifier from said proof of possession structure; and

calculating a correct key identifier from said subject public key information.

4. The method of claim 3, wherein the accuracy of said plurality of data fields is verified if:

said host name is matched with an identity of said target host system;

said extracted password is validated as a valid password for the end user; and

said extracted key identifier is matched with said correct key identifier calculated from said subject public key information.

5. The method of claim 3, wherein said extracted password and said extracted key identifier are initially symmetrically encrypted.

6. The method of claim 3, wherein said extracted password and said extracted key identifier are initially asymmetrically encrypted.

7. The method of claim 1, wherein:

said plurality of data fields includes a password; and

said signed object does not include said password.

8. A storage medium encoded with a machine readable computer program code for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, the storage medium including instructions for causing a computer to implement a method, the method comprising:

receiving, from the certification authority in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the identity of the end user, and a proof of identity possession by the end user;

analyzing the content of said plurality of data fields;

verifying the accuracy of said plurality of data fields; and

if said plurality of data fields is verified as accurate, sending a signed object to the certification authority, said signed object comprising the proof of possession confirmation.

9. The storage medium of claim 8, wherein said plurality of data fields further comprises:

a host name;

a subject identification;

a subject public key information; and

a sealed proof of possession.

10. The storage medium of claim 9, wherein analyzing the content of said plurality of data fields further comprises:

decrypting a proof of possession structure from said sealed proof of possession;

extracting a password from said sealed proof of possession structure;

extracting a key identifier from said proof of possession structure; and

calculating a correct key identifier from said subject public key information.

11. The storage medium of claim 10, wherein the accuracy of said plurality of data fields is verified if:

said host name is matched with an identity of said target host system;

said extracted password is validated as a valid password for the end user; and

said extracted key identifier is matched with said correct key identifier calculated from said subject public key information.

12. The storage medium of claim 10, wherein said extracted password and said extracted key identifier are initially symmetrically encrypted.

13. The storage medium of claim 10, wherein said extracted password and said extracted key identifier are initially asymmetrically encrypted.

14. The storage medium of claim 8, wherein:

said plurality of data fields includes a password; and

said signed object does not include said password.

15. A computer data signal for creating a proof of possession confirmation for inclusion by a certification authority into a digital certificate, the digital certificate for use by an end user, the computer data signal comprising code configured to cause a processor to implement a method, the method comprising:

receiving, from the certification authority in response to a certificate request by the end user, a plurality of data fields corresponding to a target host system, the identity of the end user, and a proof of identity possession by the end user;

analyzing the content of said plurality of data fields;

verifying the accuracy of said plurality of data fields; and

if said plurality of data fields is verified as accurate, sending a signed object to the certification authority, said signed object comprising the proof of possession confirmation.

16. The computer data signal of claim 15, wherein said plurality of data fields further comprises:

a host name;

a subject identification;

a subject public key information; and

a sealed proof of possession.

17. The computer data signal of claim 16, wherein analyzing the content of said plurality of data fields further comprises:

decrypting a proof of possession structure from said sealed proof of possession;

extracting a password from said sealed proof of possession structure;

extracting a key identifier from said proof of possession structure; and

calculating a correct key identifier from said subject public key information.

18. The computer data signal of claim 17, wherein the accuracy of said plurality of data fields is verified if:

said host name is matched with an identity of said target host system;

said extracted password is validated as a valid password for the end user; and

said extracted key identifier is matched with said correct key identifier calculated from said subject public key information.

19. The computer data signal of claim 17, wherein said extracted password and said extracted key identifier are initially symmetrically encrypted.

20. The computer data signal of claim 17, wherein said extracted password and said extracted key identifier are initially asymmetrically encrypted.

21. The computer data signal of claim 15, wherein:

said plurality of data fields includes a password; and

said signed object does not include said password.